УДК 004.056.55: 519.2

ОЦІНКИ СКЛАДНОСТІ ГЕНЕРУВАННЯ ТА ВИБОРУ ПАРАМЕТРІВ АСИМЕТРИЧНИХ АЛГОРИТМІВ

К. Д. Астаф'єва[1, a]

[1] *Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Фізико-технічний інститут*

Анотація

У роботі знаходяться теоретичні та експериментальні оцінки складності генерування і вибору параметрів асиметричних алгоритмів. Розглядається питання трудомісткості побудови основних асиметричних криптосистем.

Ключові слова: складність теоретико-числових алгоритмів, параметри асиметричних криптосистем, прості числа спеціального вигляду, тести перевірки чисел на простоту, статистичне моделювання.

Вступ

Побудова асиметричних криптосистем і протоколів потребує ретельного вибору певних параметрів, оскільки, від їх алгебраїчних і ймовірнісних властивостей залежить стійкість та ефективність криптографічного захисту інформації. Задля уникнення ряду атак такі параметри повинні мати спеціальні властивості та задовольняти певним вимогам. Причому, при виборі випадкових таємних параметрів додаткові вимоги не повинні суттєво обмежувати потужність вибіркового простору. Генерування та підбір параметрів асиметричних алгоритмів з високою криптографічною якістю є на сьогодні важливою задачею криптографічного захисту.

Основні асиметричні алгоритми використовують прості числа зі спеціальними властивостями. Зважаючи на це, постає питання вибору простих чисел та простих чисел спеціального виду з певними властивостями. Оскільки, найчастіше використовувані алгоритми перевірки чисел на псевдопростоту є ймовірнісними, то виникає питання пошук компромісу між достовірністю вибору простого числа та складністю його генерування і перевірки.

У роботі проводиться теоретичне і експериментальне дослідження складності генерування простих чисел, простих чисел спеціального виду, порівняння отриманих експериментальних і теоретичних оцінок, планується дослідження складності побудови основних криптосистем із врахуванням раніше отриманих нами результатів.

1. Теоретичні оцінки ймовірності вибору m–бітного простого числа та середньої кількості спроб до вибору простого числа

Для знаходження теоретичних оцінок складності генерування, вибору параметрів та побудови асиметричних криптосистем необхідно оцінити складність основних процедур, методів та алгоритмів, які при цьому застосовуються. Перш за все, необхідно отримати оцінки складності зверху та середні оцінки складності для таких методів і алгоритмів:

- способи генерування випадкових чисел з високою криптографічною якістю;
- алгоритми модульної арифметики;
- генерування, перевірка та вибір великих простих чисел;
- генерування, перевірка великих простих чисел спеціального виду.

1.1. Теоретичні оцінки ймовірності вибору m–бітного випадкового простого числа та середньої кількості спроб до вибору простого числа

Нехай маємо якісний генератор великих випадкових чисел, що генерує рівномірно розподілені випадкові цілі числа з інтервалу $[2^{m-1}+1, 2^{m-1}]$, тобто m–бітне число. З використанням такого генератора випадкових чисел вибираємо непарне випадкове m–бітне число. Перший та m–ий біти такого числа дорівнюють 1, кількість всіх таких чисел в інтервалі $[2^{m-1}+1, 2^{m-1}]$ дорівнює 2^{m-2}, де $2^{m-1}+1$ – мінімальне, а 2^{m-1} – максимальне число з інтервалу. Відомо, що число простих чисел $\pi(n)$ в інтервалі $[1, n]$ для великих n визначається формулою $\pi(n) \sim \frac{n}{\ln n}$, $n \to \infty$ [1]. Тоді в інтервалі $[2^{m-1}+1, 2^{m-1}]$ для великих n число простих чисел можна знайти за співвідношеннями $\pi\left(2^m-1\right) - \pi\left(2^{m-1}\right) \sim \frac{2^m-1}{\ln(2^m-1)} = \frac{2^{m-1}}{\ln 2^{m-1}} = \frac{2^{m-1}}{\ln 2}\left[\frac{2-\frac{1}{2^{m-1}}}{m\left(1+\frac{\ln\left(1-\frac{1}{2m}\right)}{m\ln 2}\right)} - \frac{1}{m-1}\right] \sim \frac{2^{m-1}}{m\ln 2}\left(1-\frac{1}{m-1}\right) \sim \frac{2^{m-1}}{m\ln 2}$

Тоді ймовірність P того, що випадково вибране непарне m – бітне число буде просте $P \sim \frac{2^{m-1}}{m2^{m-2}\ln 2} =$

[a] kateastafieva1@gmail.com

$\frac{2}{m \ln 2}$. Якщо спроби вибору випадкових чисел незалежні, то число спроб до вибору простого числа буде геометрично розподіленою випадковою величиною. Тоді середнє число спроб N_m до вибору m–бітного простого числа буде $N_m = \frac{1}{p} \sim \frac{1}{2} m \ln 2$. Наприклад, для $m = 512$ маємо, $N_{512} = 256 \ln 2 \approx 177.45$, а для $m = 1024$, відповідно, $N_{1024} = 512 \ln 2 \approx 354.89$.

1.2. Тест Міллера-Рабіна перевірки числа на простоту та генерування простих чисел спеціального виду

Застосування k разів імовірнісного тесту Міллера-Рабіна перевірки числа на простоту на k різних основах дає ймовірність помилки другого роду $\beta = 4^{-k}$ – ймовірность того, що при позитивній відповіді критерію число виявиться не простим[2].

Для запобігання відомим криптоаналітичним атакам прості числа, які використовуються в багатьох алгоритмах і протоколах асиметричної криптографії, повинні мати спеціальні властивості. Зокрема, прості числа повинні мати вигляд: $p = Cq + 1$, де q - також просте число, C - невеликий множник, зазвичай, $c = 2$ [3]. Генерація і вибір таких простих чисел проходить у два етапи: спочатку будується описаним вище способом просте число q, потім число $p = Cq+1$ перевіряється на простоту. Застосовуються також прості числа більш складного спеціального вигляду[3, 4].

2. Результати експериментального дослідження

2.1. Дослідження складності генерування та перевірки великих випадкових простих чисел

Було розглянуто декілька видів генераторів випадкових чисел, а саме вбудований java.Random для бібліотеки BigInteger, побітовий генератор, регістр лінійного зсуву, а також послідовність, що була отримана унаслідок шифрування AES(128)[3]. Згенеровані 1024-бітні випадкові числа перевірялись ймовірнісним алгоритмом Міллера-Рабіна із 64 основами. Експериментально оцінено кількість спроб до вибору простого числа з ймовірністю помилки $= 1/2^{128}$. Знаходились усереднені оцінки по вибіркам з 10, 100 та 1000 чисел та обраховувалося середнє значення кількості спроб до вибору простого числа. Результати досліджень наведені нижче.

Табл. 1. Результати знаходження кількості спроб для генерування простого числа для різних типів генераторів

	10	100	1000
java.util.Random	638.8	715.92	675.83
bitGenerator	629.6	697.61	721.429
AESGenerator	698.7	721.5	717.3
LSR	498.5	685.49	685.49

Отримані результати узгоджуються з теоретичними, отриманими за формулою $N_m = \frac{1}{2} m \ln 2$.

2.2. Дослідження складності генерування, перевірки та вибору великих випадкових простих чисел спеціального виду

Проведено статистичне дослідження для отримання експериментальних оцінок складності генерування простих чисел виду $p = 2q + 1$, де q – просте. На генераторі bitGenerator отримано результат – у середньому 423.5 спроб до вибору простого числа такого виду. Отримані результати підтверджують гіпотезу, про те що частка простих чисел виду $p = 2q + 1$, де q – просте, серед чисел такого виду у середньому більше, ніж частка простих чисел серед усіх чисел з одного інтервалу.

З використанням отриманих оцінок складності генерування, перевірки та вибору великих випадкових простих чисел та простих чисел спеціального виду можна знаходити складності побудови таких алгоритмів асиметричної криптографії як криптосистеми Діффі-Хелмана, Ель-Гамаля, RSA, Рабіна та інших[3, 4].

Висновки

У даній роботі розглянуті різні способи генерації простих чисел та простих чисел спеціального виду, що ,часто, є параметрами основних асиметричних криптосистем. Досліджена складність пошуку даних параметрів та порівняно отримані експериментальні данні із теоретичними результатами. В подальшому планується отримати оцінки генерування і вибору криптографічно якісних параметрів різних асиметричних криптосистем та трудомісткості їх побудови із врахуванням вищенаведених методів і даних.

Перелік використаних джерел

1. К. Прахар. Распределение простых чисел. — Мир, 1967. — С. 512 с.
2. М. Глухов М., Б. Пичкур А., В. Черемушкин А. Введение в теоретико-числовые методы криптографии: Учебное пособие. — Лань, 2011. — С. 816 с.
3. Б. З. Шнайер. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке СИ. — ТРИУМФ, 2003.
4. А. Тилборг Ван Х. К. Основы криптологии. Профессиональное руководство и интерактивный учебник. — Мир, 2006.